

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES	)	
	)	
v.	)	No. 11-10260-NMG
	)	
AARON SWARTZ	)	
_____	)	

DEFENDANT AARON SWARTZ'S MOTION FOR DISCOVERY

On May 8, 2012, defendant Aaron Swartz sought from the government 21 enumerated categories of discovery from the government. *See* Exhibit A, submitted herewith. That request was followed by a letter dated May 10, 2012, outlining the bases for the requests made in the earlier letter. *See* Exhibit B, submitted herewith. Following discussions by the parties conducted in good faith to eliminate and/or narrow the areas of dispute, the government responded to Swartz's discovery requests on May 18, 2012. *See* Exhibit C, submitted herewith. This motion requests that the government be ordered to provide Swartz with the discovery which it has declined to produce: that described in paragraphs 1, 4, 6, 12, 15, and 20 of Swartz's May 8, 2012, discovery request letter.

I. PARAGRAPH 6.

This paragraph requested that the government provide "[a]ny and all notes and reports provided to USSS or USAO by CERT in relation to their forensic analysis of the ACER laptop, or of any analysis of any other evidence including but not limited to the PCAP log information sent to CERT by the USSS for analysis." "CERT" in this request refers to the Carnegie Mellon computer response team which provides assistance to the USSS with complex computer and internet issues.

In this case, CERT conducted analyses, which it provided to the United States Attorney's Office, of MIT computer/internet information relating to Swartz's alleged use of the MIT system and/or of certain computers or hard drives which the government associates with Swartz. Information received in discovery indicates that the flow traffic on MIT's network was being contemporaneously uploaded to the CERT "dropbox." The government has declined to provide these reports and other information on the ground that no CERT personnel will be appearing as expert witnesses at the trial of this case and that, if they do, such discovery should be subject to the separate schedule for the disclosure of reports of experts rather than to the obligations relating to disclosure of scientific results or tests. That fact, however, does not eliminate the defendant's entitlement to this information. Swartz is entitled to the production of reports of scientific tests under Fed. R. Evid. 16(a)(1)(F), which entitles the defendant to the "results or reports" of "any scientific test or experiment" if the item is in the possession of the government – as it is here – and if the item is material to the preparation of the defense *or* the government intends to use the item in its case-in-chief at trial. Rule 16(a)(1)(F) encompasses forensic examination of computer/internet data or information. *See, e.g., United States v. Pires*, 2009 WL 2176664 at *1 (D.Mass. July 22, 2009); *United States v. Robinson*, 2006 WL 468298 at *4 (N.D.Tex. Feb. 28, 2006). Here, the requested information is material to the preparation of Swartz's defense and to Swartz's potential ability to file a particularized motion to suppress asserting violations of 18 U.S.C. §2510 *et seq.* and/or the Fourth Amendment.

II. PARAGRAPH 12.

This paragraph requested that the government provide:

As to the ACER laptop: the dates of any searches (defined as any attempt to see any information contained on the computer that would not be visible without touching the computer in any way including but not limited to any port scan of the computer, any imaging

of the laptop or any portion of its contents, any powering or opening of any file or folder or data contained in the laptop, any touching of a key or moving of a mouse so as to put in view new information, and any analysis or review by CERT or USSS of any of the contents of the laptop whether obtained remotely, by a physical search, or by a search of an image of the laptop), the identity of each individual who conducted any search of the laptop computer, the date of such search and the legal basis for each such search.

The government has provided Swartz with the February, 2011, search warrant authorizing the search of an ACER laptop alleged to have been used by Swartz in relation to the events which are the subject of the indictment in this case. However, Swartz has information indicating that the government attempted to gain access to the contents of the laptop and/or to modify the condition of the ACER laptop on January 6, 2011, the date of its seizure, and possibly at other times prior to the execution of the search warrant. Moving a mouse or touching a key on a computer which reveals information that was not in plain view constitutes a search which may not be lawfully conducted under the Fourth Amendment in the absence of a valid warrant. *See, e.g., United States v. Musgrove*, 2011 WL 4356515 at *15 (E.D.Wis. September 16, 2011); *see also Arizona v. Hicks*, 480 U.S. 321 (1987). The requested information is critical to Swartz's ability to prepare a particularized motion to suppress unlawfully obtained evidence or other information if such incursions or attempted incursions into the contents of the laptop were made in the absence of a validly issued search warrant.

III. PARAGRAPH 15.

This paragraph asked the government to "identify the origin of any and all statements of Aaron Swartz including but not limited to emails, text messages, chats, documents, memoranda or letters, i.e., to identify the source from which each statement was received and the legal procedure used to obtain each such statement of the defendant." Swartz has received in discovery internet

memoranda and chats purporting to be from him. For example, the discovery contains a number of chats on googlegroups.com which contain entries which facially indicate that Swartz was a participant in the communications. The discovery also contains a number of emails which on their faces indicate that they were either to or from Swartz. Swartz requires the additional information requested – the source of these statements and the procedure used by the government to obtain them – to enable him to move to suppress such statements if grounds exist to do so, which he cannot determine without the requested information. *See* Fed. R. Crim. P. 12(b)(4).

IV. PARAGRAPHS 1, 4, 20.

These paragraphs request information relating to grand jury subpoenas. Paragraph 1 requested that the government provide “[a]ny and all grand jury subpoenas – and any and all information resulting from their service – seeking information from third parties including but not limited to Twitter, MIT, JSTOR, Internet Archive that would constitute a communication from or to Aaron Swartz or any computer associated with him.” Paragraph 4 requested “[a]ny and all SCA applications, orders or subpoenas to MIT, JSTOR, Twitter, Google, Amazon, Internet Archive or any other entity seeking information regarding Aaron Swartz, any account associated with Swartz, or any information regarding communications to and from Swartz and any and all information resulting from their service.” Paragraph 20 requested “[a]ny and all paper, documents, materials, information and data of any kind received by the Government as a result of the service of any grand jury subpoena on any person or entity relating to this investigation.”

Swartz requests this information because some grand jury subpoenas used in this case contained directives to the recipients which Swartz contends were in conflict with Rule 6(e)(2)(A), *see United States v. Kramer*, 864 F.2d 99, 101 (11th Cir. 1988), and others sought certification of

the produced documents so that they could be offered into evidence under Fed. R. Evid. 803(6), 901. Swartz requires the requested materials to determine whether there is a further basis for moving to exclude evidence under the Fourth Amendment (even though the SCA has no independent suppression remedy).

The Fourth Amendment “provides protection against a grand jury subpoena too sweeping in its terms “to be regarded as reasonable.”” *United States v. Dionisio*, 410 U.S. 1, 11 (1973), *quoting Hale v. Henkel*, 201 U.S. 43, 76 (1906). *See United States v. Calandra*, 414 U.S. 338, 346 (1974)(“A grand jury’s subpoena duces tecum will be disallowed if it is ‘far too sweeping in its terms to be regarded as reasonable’ under the Fourth Amendment”); *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973)(“the Constitution undoubtedly protects against overly broad *subpoenas duces tecum*”); *In re Eight Grand Jury Subpoenae Duces Tecum*, 701 F.Supp. 53, 55 (S.D.N.Y. 1988)(grand jury “may not issue a subpoena so broad as to impinge unreasonably on legitimate fourth amendment rights”); *In re Grand Jury Subpoenas Served Feb. 27, 1984*, 599 F.Supp. 1006, 1017 (E.D. Wash. 1984)(“There is no doubt that a grand jury subpoena *duces tecum* must pass constitutional muster”). Swartz retains a reasonable expectation of privacy in his emails and chat communications even though they are in the hands of a third party internet service provider. *See United States v. Warshak*, 631 F.3d 266, 283-87 (2010).

Moreover, defendant believes that the items would not have been subpoenaed by the experienced and respected senior prosecutor, nor would evidentiary certifications have been requested, were the subpoenaed items not material to either the prosecution or the defense. Defendant’s viewing of any undisclosed subpoenaed materials would not be burdensome, and disclosure of the subpoenas would not intrude upon the government’s work product privilege, as the

subpoenas were served on third parties, thus waiving any confidentiality or privilege protections.

Respectfully submitted,

By his attorney,

/s/ Martin G. Weinberg

Martin G. Weinberg

20 Park Plaza, Suite 1000

Boston, MA 02116

(617) 227-3700 (tel.)

(617) 338-9538 (fax)

owlmgw@att.net

CERTIFICATE OF SERVICE

I, Martin G. Weinberg, hereby certify that on this 1st day of June, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA.

/s/ Martin G. Weinberg

Martin G. Weinberg

Swartz
Carr

MARTIN G. WEINBERG, P.C.
ATTORNEY AT LAW

20 PARK PLAZA, SUITE 1000
BOSTON, MASSACHUSETTS 02116

(617) 227-3700

FAX (617) 338-9538

NIGHT EMERGENCY:
(617) 901-3472

EMAIL ADDRESSES:

owlmcb@att.net
owlmgw@att.net

May 8, 2012

Stephen Heymann
Assistant United States Attorney
United States Attorney's Office
1 Courthouse Way
Boston, MA

RE: United States v. Aaron Swartz

Dear Mr. Heymann:

This letter is authored to request that you provide me with the following discovery that is material to the preparation of the above-captioned matter:

1. Any and all grand jury subpoenas – and any and all information resulting from their service - seeking information from third parties including but not limited to Twitter, MIT, JSTOR, Internet Archive that would constitute a communication from or to Aaron Swartz or any computer associated with him;
2. Any and all grand jury subpoenas – and any and all information resulting from their service - seeking information regarding the defendant wherein the receiver of the subpoena is warned that disclosure to third parties would or could or might impede the investigation or containing any indirect or direct references that disclosure might impede or obstruct a criminal investigation;
3. Any and all grand jury subpoenas – and any and all information resulting from their services – which contain a request for a certificate of authenticity and/or a certificate wherein a record keeper or representative of the entity receiving the subpoena affirms information about the produced records that would meet either hearsay or authenticity evidentiary challenges;
4. Any and all SCA applications, orders, or subpoenas to MIT, JSTOR, Twitter, Google, Amazon, Internet Archive, or any other entity seeking information regarding

Aaron Swartz, any account associated with Swartz, or any information regarding communications to and from Swartz and any and all information resulting from their service;

5. Any and all preservation letters sent to MIT in relation to this investigation that require that MIT preserve the results of all recorded or captured router data resulting from MIT's utilization of programs or hardware to create tcpdump formatted files beginning no later than 11-7-2010;

6. Any and all notes and reports provided to USSS or USAO by CERT in relation to their forensic analysis of the ACER laptop, or of any analysis of any other evidence including but not limited to the PCAP log information sent to CERT by the USSS for analysis;

7. Any and all fingerprint reports comparing the known prints of Aaron Swartz or any other person with any latent or unknown prints lifted from any evidence in relation to this case (other than such reports that were already disclosed);

8. Any and all telephone toll records subpoenaed or otherwise obtained in relation to this case;

9. Any and all credit card statements or account information subpoenaed or otherwise obtained in relation to this case;

10. Any and all documents reflecting the purchase of computers or computer software or external hard-drives that are material to this case;

11. Any and all Grand Jury testimony provided on or about 6-16-11 and any memoranda of interview of Quinn Norton;

12. As to the ACER laptop: the dates of any searches (defined as any attempt to see any information contained on the computer that would not be visible without touching the computer in anyway including but not limited to any port scan of the computer, any imaging of the laptop or any portion of its contents, any powering or opening of any file or folder or data contained in the laptop, any touching of a key or moving of a mouse so as to put into view new information, and any analysis of review by CERT or USSS of any of the contents of the laptop whether obtained remotely, by a physical search, or by a search of an image of the laptop), the identity of each individual who conducted any search of the laptop computer, the date of such search and the legal basis for each such search;

13. As to any evidence seized from the backpack of the defendant on January 6, 2011, the same requests as in paragraph 12, supra;

14. Any and all chain of custody reports from USSS and other federal entities regarding any intended government exhibit;

15. To identify the origin of any and all statements of Aaron Swartz including but not limited to emails, text messages, chats, documents, memoranda or letters ie. to identify

the source from which each such statement was received and the legal procedure used to obtain each such statement of the defendant as required by FRCrimP 12(d)(1);

16. Any and all information including but not limited to 70 gigabytes or more of historical network flow data dating from 12-14-10 through 1-6-11 and all DHCP log information provided to S/A Pickett by MIT employees including but not limited to Michael Halsall (see log pg 7) to the extent that such flow data, radius logs, network capture data and DHCP log information was not provided to the defendant on or about November 18, 2011;

17. Any and all additional (a) IP connection logs and/or DHCP logs, (b) radius logs, (c) flow data files, and (d) network capture files that the USSS or any other federal entity received from MIT or JSTOR (some but not all of such logs were provided to the defense and this request is for any other such logs, network capture files, or flow data that was received from MIT or JSTOR in connection to this investigation regardless of whether it was associated with IP addresses alleged to have been used by the defendant);

18. Any and all additional documents, reports, data, or other information received from MIT or JSTOR that is outside paragraphs 16 and 17 and not previously provided to the defendant in discovery and the legal vehicle if any which resulted in the transmission of such information to the Government;

19. As to any MAC addresses that the Government associates with the defendant, when was information about each received, from who, pursuant to what process;

20. Any and all paper, documents, materials, information, and data of any kind received by the Government as a result of the service of any grand jury subpoena on any person or entity relating to this investigation; and

21. Any and all paper, documents, materials, information and data of any kind received by the Government from the Middlesex District Attorney or any state or city law enforcement authority that resulted from the service of any state grand jury subpoena on any person or entity relating to this investigation

If you believe that you have already provided me with the entirety of the materials requested in any paragraph, please so inform me. If you believe that you have provided me with some but not all of the requested information, please provide the remainder. If you want to discuss the basis for these requests, beyond the requirements of Rule 16 and corresponding Local Rules, please advise as to which paragraphs.

Yours Truly,

Martin G. Weinberg, Esq.

MARTIN G. WEINBERG, P.C.
ATTORNEY AT LAW

20 PARK PLAZA, SUITE 1000
BOSTON, MASSACHUSETTS 02116

(617) 227-3700

FAX (617) 338-9538

NIGHT EMERGENCY:
(617) 901-3472

EMAIL ADDRESSES:

owlmcb@att.net
owlmgw@att.net

May 10, 2012

Stephen Heymann
Assistant United States Attorney
United States Attorney's Office
1 Courthouse Way
Boston, MA

RE: *United States v. Aaron Swartz*

Dear Mr. Heymann:

You have requested that I supplement my letter to you dated May 8, 2012, by disclosing the legal basis for my requests contained therein.

1. As to paragraphs 1, 2, 3, 8, 9, 10, 18, 20, and 21, the objective is to discover information and inspect papers and documents within the Government's possession that are material to preparing the defense in this case, see Fed. R. Crim. P. 16(a)(1)(E)(i). The presupposition for each paragraph is that I am seeking documentary evidence that you subpoenaed or otherwise acquired from third parties in relation to this investigation. Given that you would not issue overbroad subpoenas, I would assume that what you were provided was material to the investigation and hence to the defense for this matter. As to paragraph 1, I am also seeking information pursuant to Rule 16(a)(1)(A) and, to the extent you received emails or other communications of the defendant that were stored for him by a third party, I rely on Rule 16(a)(1)(E)(iii). As to paragraph 2, I believe full discovery is the minimal response to the inappropriate threat that is on the face of at least one of your grand jury subpoenas. See, e.g. *United States v. Kramer* 864 F.2d 99, (11th cir. 1988). As to paragraph 3, I rely upon Rule 16(a)(1)(E)(i),(ii).

2. As to paragraphs 4, 5, 12, 13, 14, 16, 17, and 19, I rely on Rule 16(a)(1)(E)(i),(iii) and in particular on the relationship between such requested discovery and Mr. Swartz' rights to protect his Fourth Amendment and Title III rights in this case. I also invoke Fed. R. Crim. P. 12(b)(4): although the rule is literally confined to evidence you intend to

use (I would request that you make this disclosure), I would need as well to determine if the February, 2011, court authorized searches were tainted by the January, 2011, warrantless searches.

3. As to paragraph 11, *Brady v. Maryland*, 373 U.S. 83 (1963).
4. As to paragraph 15, Rule 16(a)(1)(B).
5. As to paragraphs 6 and 7, Rule 16(a)(1)(F).

I think a paragraph by paragraph review of the requests and your proposed responses prior to our need to draft a status conference report for May 22, 2012, makes sense.

Thanks,

Martin G Weinberg, Esq.



U.S. Department of Justice

Carmen M. Ortiz
United States Attorney
District of Massachusetts

Main Reception: (617) 748-3100

John Joseph Moakley United States Courthouse
1 Courthouse Way
Suite 9200
Boston, Massachusetts 02210

May 18, 2012

Martin G. Weinberg
20 Park Plaza
Suite 1000
Boston, MA 02116

Re: U.S. v. Aaron Swartz

Dear Mr. Weinberg:

This letter formalizes in accordance with Local Rule 116.3(a) my response to your letter request for additional discovery dated May 8, 2012. I found our lengthy discussions on Tuesday concerning your various requests very helpful in identifying and narrowing those areas in which we have meaningful disagreements that will need to be considered and resolved by the court.

We have previously provided to you and your predecessor counsel not only all material described in Federal Rule of Criminal Procedure 16 and Local Rules 116.1 and 116.2 as being appropriate at this stage of the criminal case, but also an extensive body of email, computer logs, law enforcement reports, photographs and video recordings created and concerning the events and investigation leading to your client's arrest in the organized form of a Concordance database. Except as set forth below, we cannot agree to furnish the materials which you have requested to the extent that they go beyond the very large body of materials which we have already produced which already far exceed those required by the local and federal rules, and the statutes and constitutional provisions they embody. We cannot see how many of the materials you have requested are material to the defense and many others, as we discussed, are either privileged or will be furnished at later times as specified by the Court, rules and governing statutes.

In light of our useful discussions, and again in the hope of narrowing those potential discovery disputes which the court will need to resolve, this letter will also serve to confirm the following aspects of our discussions:

1. A central focus of our discussions were suppression remedies you potentially thought you might pursue. As you are aware, there is no suppression remedy under the Stored Communications Act. *See* 18 U.S.C. § 2708. To the extent that you believe it was necessary to

Martin G. Weinberg
May 18, 2012
Page 2

obtain a warrant under Rule 41 of the Federal Rules of Criminal Procedure or 18 U.S.C. §2703 before conducting a particular search, copies of all warrants obtained during the investigation of this case were provided to your predecessor counsel on August 12, 2011. I understand that all of these were transferred to you when you took over the case, but, if not, please do not hesitate to let me know and I will forward a second set to you.

2. You previously have been provided with all MIT logging data in the government's possession pertaining to your client relevant to this case. The government received from MIT additional RADIUS logs which the government has been informed pertain only to third parties who happened to have plugged into MIT's computer network on January 6, 2011 as well. Based on your representation that the third-party logging information is material to the defense of this case, the government has no objection to providing to you the additional logs, subject to paragraph 2(a)(v)(b) of the Protective Order entered in this case.

3. You have previously been provided all reports of fingerprint examinations conducted during the federal investigation of this case.

4. In keeping with Local Rule 116.8, we have sought to obtain any information subject to disclosure from all federal, state and local law enforcement agencies formally participating in the criminal investigation that resulted in this case.

Yours very truly,

CARMEN M. ORTIZ
United States Attorney

By:


STEPHEN P. HEYMANN
Assistant U.S. Attorney